IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff(s), vs. DOMINIC DZWONCZYK, Defendant(s).	No. 4:15-CR-3134 BRIEF IN SUPPORT OF OBJECTION TO THE MAGISTRATE JUDGE'S FINDINGS, RECOMMENDATION AND ORDER

TABLE OF CONTENTS

FACTS

Defendant filed a Motion to Suppress on May 6, 2016 seeking to suppress all information acquired as a result of an unlawful search conducted pursuant to an NIT warrant. The NIT warrant authorized the government to deploy a software program (malware), from a server located in the Eastern District of Virginia, to any computer that accessed the website hosted by the server. The malware would then infiltrate the accessing computer, unbeknownst to the user, and relay private information back to the government.

On July 11, 2016, the Government filed a Brief in Opposition to Defendant's suppression motion. Defendant filed a reply brief on September 2, 2016. During the pendency of this motion, many other cases and rulings regarding this same NIT warrant have been ruled upon by other United States District Courts. In its Findings, Recommendation and Order (hereinafter referred to as "FRO") the Magistrate has recommended Defendant's Motion be denied.

ARGUMENT

The Magistrate Judge has suggested that Defendant did not have a reasonable expectation of privacy in the information that was obtained as a result of the NIT warrant and the warrant itself was valid. Moreover, the Magistrate Judge has purported that ***even if the warrant was invalid***, suppression is not the appropriate remedy. See FRO, p. 14, ¶1; p.16, ¶2. Defendant respectfully objects.

1. The Court erred in determining that the Defendant did not have a reasonable expectation of privacy.

When the Court considers the issue of Defendant's reasonable expectation of privacy, the question becomes whether the IP address should be the focus of this analysis or whether Defendant's expectation of privacy in his computer is the proper subject of this analysis…The courts which have thus far

> grappled with the extent to which a person has a reasonable expectation of privacy in an IP address have analyzed the issue in the context of a subpoena to an ISP to identify the person assigned the IP address. To the extent [other Courts have] concluded that an individual waives his or her expectation of privacy in his or her computer by connecting to the Tor network, this Court disagrees with that conclusion as having improperly conflated the expectation of privacy associated with an IP address with the expectation of privacy one has in the computer searched by the NIT. *U.S. v. Adams*, WL 4212079, *4 (M.D. Florida 8/10/16) (emphasis added).

As indicated in the Magistrate's Order, "Defendant's IP address was obtained using a NIT which prompted Defendant's computer to reveal the actual IP address, and not through a subpoena served on a third-party internet service provider." FRO, p. 7, ¶2 (citing *U.S. v. Wheelock*, 772 F.3d 825 (8th Cir. 2014)). This very language differentiates the expectation of privacy in one's IP address when it is obtained ***through*** a third-party rather than ripped directly from the user's computer. The Magistrate has suggested that since there is no expectation of privacy in one's IP address, it does not matter how that information was obtained. See FRO, p. 7, ¶2 ("If the sole question was whether a Defendant has a reasonable expectation of privacy in his IP address, applying Eighth Circuit law, the answer would simply be 'No'.")

The Honorable Judge Robert Pratt in the Southern District of Iowa in *U.S. v. Croghan*, 2016 WL 4992105 (S.D. Iowa 9/19/2016), brought up the fallacy of this misguided logic in discussing the distinction between the government seizing Defendant's IP address from his home computer rather than his internet provider. *Id.* *7.

> There is a significant difference between obtaining an IP address ***from a third party*** and obtaining it ***directly from a defendant's computer***…If a defendant writes his IP address on a piece of paper and places it in a drawer in his home, there would be no question that law enforcement would need a warrant to access that piece of paper – even accepting that the defendant had no reasonable

> expectation of privacy in the IP address itself. Here, Defendants' IP addresses were stored on their computers in their homes rather than in a drawer. *Id*. (emphasis in original)

As Judge Pratt has elaborated, it is the method of obtainment that should dictate the expectation of our privacy. For instance, owning a phone that is assigned a phone number by a service provider does not give the government justification for breaking down one's door, entering one's home and seizing the phone purely for the purpose of retrieving the phone number. Then, when confronted with the issue of the illegal intrusion into the home, simply shrugging their shoulders and suggesting no wrongdoing occurred since they only conducted the illegal entry and search to obtain the phone number; something that we have no expectation of privacy in anyway. See *U.S. v. Workman*, 2016 WL 5791209, *6 (D. Colo. 9/6/16) (holding that the "government is not permitted to conduct a warrantless search of a place in which a defendant has a reasonable expectation of privacy simply because it intends to seize property for which the defendant does not have a reasonable expectation of privacy."), *U.S. v. Adams*, 2016 WL 4212079 (M.D. Florida, 8/10/16) ("The NIT searches the user's computer to discover the IP address associated with that device. Therefore, ***one's expectation of privacy in that device is the proper focus of the analysis, not one's expectation of privacy in the IP address residing in that device***. For example, a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage.") (emphasis added).

In Defendant's case, the Government has admitted it had absolutely no way to obtain his IP address from his Internet Service Provider. Instead, the Government could only rely on the unlawful intrusion into his home through malicious, hidden software and obtain (unbeknownst to him)

not only his IP address, but other identifying information regarding his computer (Media Access Control, Operating System, computer hostname and username). The Government now attempts to justify the intrusion by claiming that nobody has an expectation of privacy in such information. Regardless of the information sought or the expectation of privacy in that information, a valid warrant was required to obtain the information directly from Defendant's home computer. This would be a different analysis and different result if the Government had sought this information from a third party provider. However, here, the Government has obtained this information by illegally searching and seizing information contained on Defendant's computer.

2. The Court erred in determining that the deployment of the NIT onto Defendant's computer was not a "search" of the Defendant's computer.

Although the Magistrate Judge concluded that Defendant has no expectation of privacy in his IP address, the Court does recognize that Defendant has a privacy interest "in his home and its contents." FRO, p. 9, ¶1. However, the Court determined that the deployment of the NIT was not a "search" of Defendant's computer and therefore not subject to Fourth Amendment analysis. In attempting to justify this holding, the Magistrate admitted that Defendant's computer was "compelled" by the NIT to send information to law enforcement. FRO, p. 9, ¶2 ("Thus, the NIT essentially compelled Defendant's computer to produce its IP address (similar to a return address on an envelope) when the NIT instructed the computer to send other information identified in the Virginia Warrant.").

To conclude that Defendant's computer wasn't searched because it was only "compelled" and "instructed" to "produce" and "send" information to law enforcement is confounding. The NIT searched (i.e. compelled,

manipulated, forced, coerced, obligated, instructed, commanded) Defendant's computer to obtain information.

Whichever synonym the Court chooses to use, it is undisputed that the NIT infiltrated the Defendant's computer, obtained information contained in that computer, and provided it to law enforcement. The Defendant had an expectation of privacy in his computer and his computer was unlawfully searched by the deployment of the NIT.

3. The Court erred in holding that the NIT was a "tracking device" installed within the Eastern District of Virginia and was therefore a valid warrant issued pursuant to Fed. R. Crim. P. 41(b)(4).

The Magistrate has concluded that the NIT warrant was valid because the NIT falls under the definition of a "tracking device" pursuant to Rule 41(b)(4). (FRO, pp. 12-13). The magistrate surmised that the NIT warrant did not exceed the territorial limits of Rule 41 since "the NIT does not fit traditional notions of how tracking devices are installed or attached because internet crime and surveillance defy traditional notions of place." (FRO, pp. 12-13) (citations omitted). Since Rule 41(b)(4) requires that the tracking device be installed "within the district" and Defendant and his computer remained at all times in the District of Nebraska, the Court determined that Defendant's computer made a "virtual trip" to the Eastern District of Virginia, where the NIT was then installed on his computer. This conclusion is contrary to Rule 41 and the facts present in this case.

> ***The [NIT] warrant authorizes the installation of the NIT onto the government-controlled Playpen server and not onto Defendant's computer***, which is located outside of the Eastern District of Virginia. ***Moreover, the NIT does not track; it searches***…the NIT is designed to search the user's computer for certain information, including the IP address, and to transmit that data back to a server controlled by law enforcement. *U.S. v. Adams*, 2016 WL4212079 (M.D. Florida 8/10/16) (citing *U.S. v. Michaud*, 2016 WL 337263 (W.D. Wash. 1/28/16), *U.S. v. Levin*, 2016 WL

1589824 (D. Mass. 5/5/16), *U.S. v. Arterbury*, 2016 U.S. Dist. LEXIS 67091 (N.D. OK 4/25/2016)) (emphasis added).

If the Magistrate's rationale is correct, then the limitations set forth in Rule 41 limiting territorial authority are erased by the ubiquity of the internet. Accessing the internet allows you to "virtually" travel anywhere at any moment, or allow you to be in multiple places at once (almost every web browser allows multiple windows/tabs to be open at the same time). Essentially, by accessing the internet (i.e. the World Wide Web), you are availing yourself to the world. No territorial limits exist within cyberspace, therefore, any magistrate in any district could theoretically authorize the installation of "tracking devices" on any computer anywhere.

For example, Google, one of the largest search engines and most used websites in the world, has data centers and servers located in at least 15 cities across the world, 9 alone in the United States with one of those located in Council Bluffs, Iowa. https://www.google.com/about/datacenters/inside/locations/index.html. If simply accessing the Google website means one takes a "virtual trip" to cities and states hosting the Google datacenters and servers, one has managed to be in 15 places (districts) at once and subjected themselves to the jurisdiction of each, all without necessarily knowing where they have "virtually" been. A virtual trip can be made anywhere and at any time in this digital age; that cannot mean our electronic devices are subject to the territorial jurisdictions of "everywhere." See *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 758 (S.D. Tex. 2013) (rejecting government's request to deploy software similar to the NIT because "there is no showing that the installation of the 'tracking device' (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet.").

The Magistrate from the Eastern District of Virginia exceeded her authority in authorizing a warrant that essentially had no territorial restrictions and therefore could not comply with Rule 41(b). The tracking device was installed on Defendant's computer, located at all times in the District of Nebraska. Claiming that accessing the website which was hosted by the server located in the magistrate's district was sufficient to comply with Rule 41, renders the rule meaningless. The warrant sought to search items outside of the magistrate's district, which she did not have authority to do. Because the Magistrate had no authority to issue the warrant, the warrant was not valid.

4. The Court erred by finding that even if the NIT warrant was not valid, suppression is not appropriate.

Once a court determines that a Rule 41 violation has occurred, it must next determine whether that specific Rule 41 violation rises to the level of a Fourth Amendment violation. *U.S. v. Krueger*, 809 F.3d 1109 (10th Cir. 2015). If it does, the violation can be considered constitutional and suppression is warranted without further evidence of prejudice or reckless disregard. *Id*.

A. The NIT warrant was void *ab initio* and suppression is necessary**.**

Defendant argues that the NIT warrant was void "*ab initio*." See *U.S. v. Houston*, 965 F.Supp.2d 855, 902 n.12 (E.D. Tenn. 2013) ("A search warrant issued by an individual without legal authority to do so is 'void *ab initio*'") (quoting *U.S. v. Master*, 614 F.3d 236, 241 (6th Cir. 2010)). A fundamental violation that mandates suppression because the Magistrate who signed the warrant had no authority to do so. At least three courts reviewing the NIT warrant have reached this conclusion. See *U.S. v. Levin*, 2016 WL 2596010 (D. Mass. 5/5/16); *U.S. v. Arterbury*, 2016 U.S. Dist.

LEXIS 67091 (N.D. OK 4/25/2016); *U.S. v. Croghan*, 2016 WL 4992105 (S.D. Iowa 9/19/2016).

Rule 41 has both procedural and substantive provisions and the difference matters. The violation here is not a "technical" violation of Rule 41, but involves substantial constitutional protections. See *U.S. v. Williamson*, 439 F.3d 1125, 1133 (9th Cir. 2006) (distinguishing between Rule 41 violations that are "mere technical error" and those rising to a degree of "constitutional magnitude."). The Seventh Circuit has explained that "Rule 41(b) deals with substantive judicial authority – not procedure." *U.S. v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008). In *Levin*, the court found the Rule 41 violation triggered the substantive protections of the rule because the error involved "the authority of the magistrate judge to issue the warrant" rather than simply "the procedures for obtaining and issuing warrants." *Levin*, 2016 WL 2596010, at *7-8. Because the NIT warrant was not authorized by Rule 41, it was void *ab initio*. Suppression is therefore mandated without the need for further analysis.

B. Even a non-constitutional violation of Rule 41 would necessitate suppression because Defendant was prejudiced by the violation**.**

Even if, however, only a technical/procedural violation of Rule 41 occurred, suppression would be appropriate because the Defendant was prejudiced by the violation. A Rule 41 violation amounts to a violation of the Fourth Amendment warranting exclusion "if a defendant is prejudiced or if reckless disregard of proper procedure is evident." *U.S. v. Spencer*, 439 F.3d 905, 913 (8th Cir. 2006).

The Government conceded in its application for the NIT warrant that it had no other way to obtain defendant's IP address or identifying information. *See* Brief in Support of Motion to Suppress, p. 8 (citing Ex. B, p. 28) (setting forth that if the NIT could be characterized as a seizure,

"such a seizure is reasonably necessary, ***because without this seizure, there would be no other way, to my knowledge, to view the information [IP address, etc.] and to use it to further the investigation***.") (emphasis in original). Defendant was prejudiced because without the NIT warrant the Government would not have obtained Defendant's identifying information and subsequently been able to obtain the evidence it seized pursuant to the search warrant of Defendant's residence. See *Levin*, 2016 WL 2596010 at *9 n. 16 (finding that "the government might not have obtained the evidence it seized pursuant to the Residential Warrant, since the application for that warrant was based on information it acquired through the execution of the NIT warrant."), But for the unlawful search of Defendant's computer by the NIT, the search of Defendant's residence would have never occurred.

The Magistrate has adopted the position that Defendant was not prejudiced, because "had the FBI interpreted Rule 41 as prohibiting a Virginia magistrate judge from issuing the Virginia warrant, it could have presented the application to a district judge in the Eastern District of Virginia. Defendant's IP address would have still been revealed and the Nebraska warrant would still have been supported by probable cause." FRO, p. 16, ¶2. This exact argument was dealt with, appropriately, by the Tenth Circuit in *U.S. v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), where the Circuit Court determined that a Rule 41 violation prejudiced the defendant and rejected the government's argument that it could have had a judge with appropriate authority issue the warrant, by noting that "such hypotheticals simply cannot cure the Government's gross negligence in failing to comply with Rule 41(b)(1) in the first instance." *Id*. at 1117.

Here the Government should not be allowed to argue in hindsight that they "could have had" other ways of obtaining the warrant so it ultimately doesn't matter how they obtained the information anyway. This

Court should not engage in such hypotheticals. But for the unlawful NIT warrant, the search of Defendant's computer and residence would not have occurred. This prejudiced Defendant and requires suppression of the results of the NIT warrant and all resulting fruit of the poisonous tree.

C. The *Leon* good-faith exception is not applicable**.**

Lastly, the Magistrate found that even if a violation occurred, technical or otherwise, the *Leon* good faith exception would preclude suppression. First, as previously argued by Defendant, the fact that the NIT warrant was void from the beginning should preclude a good-faith analysis as such an exception cannot apply to a void warrant. See *U.S. v. Scott*, 260 F.3d 512, 513 (6th Cir. 2001) (holding "we are confident that *Leon* did not contemplate a situation where a warrant is issued by a person lacking the requisite legal authority."). This argument was best set forth by the Honorable Judge William Young of the District of Massachusetts who explains:

> Because a warrant that was void at the outset is akin to no warrant at all, cases involving the application of the good-faith exception to evidence seized pursuant to a warrantless search are especially instructive. In *U.S. v. Curzi*, 867 F.2d 36 (1st Cir. 1989), the First Circuit declined to "recognize [ ] a good-faith exception in respect to warrantless searches." *Id*. at 44. To hold that the good-faith exception is applicable here would collapse the distinction between a voidable and a void warrant. But this distinction is meaningful: the former involves "judicial error," such as "misjudging the sufficiency of the evidence or the warrant application's fulfillment of the statutory requirements," while the latter involves "judicial authority," i.e. a judge "act[ing] outside of the law, outside of the authority granted to judges in the first place." *State v. Hess*, 320 Wis.2d 600 (Ct. App. Wis. 2009)…Were the good-faith exception to apply here, courts would have to tolerate evidence obtained when an officer submitted something that reasonably looked like a valid warrant application, to someone who, to the officer, appeared to have authority to approve that warrant application…This court holds that such an expansion of the good-faith exception is improvident, and not required by precedent. *U.S. v. Levin*, 2016 WL 2596010 at *12.

This rationale was also adopted and echoed by United States District Court Judge R. Brooke Jackson of the District of Colorado, when he stated, "where the issuing judge acts outside of her authority the good-faith exception should not apply." *U.S. v. Workman*, 2016 WL 5791209, *8 (D. Colo. 9/6/16).

In response to the Court's statement that "Defendant has provided no evidence indicating the Virginia Warrant lacked a showing of probable cause or judicial authority such that a reasonable officer would not have relied upon it", FRO, p. 19, ¶3, Defendant submits the following quote from the Honorable Judge Young of the District of Massachusetts:

> Even were the Court to hold that the good-faith exception *could* apply to circumstances involving a search pursuant to a warrant issued without jurisdiction, it would decline to rule such exception applicable here. For one, it was not objectively reasonable for law enforcement – particularly a veteran FBI agent with 19 years of federal law enforcement experience, to believe that the NIT Warrant was properly issued considering the plain mandate of Rule 41(b). See *U.S. v. Glover*, 736 F.3d 509, 516 (D.C. Cir. 2013) ("[I]t is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by 'good faith'."). *U.S. v. Levin*, 2016 WL 2596010 at *13.

The officers and Government officials seeking the approval of the NIT warrant knew that they were asking a Magistrate Judge to authorize a search and seizure outside of their jurisdiction. Although the Magistrate may have taken issue with Defendant's use of the word "clearly" in determining if the issuing Magistrate understood the limitations defined in Rule 41, the language of the rule itself is unambiguous and should be given its plain meaning. Knowledge of the law and its limitations would appear to negate any *Leon* reliance in a situation where a court exceeds its defined authority in issuing a warrant.

The pleadings and affidavits make it clear that law enforcement officers knew they were requesting the Magistrate to authorize a warrant for searches outside of her jurisdiction and the Magistrate should have known she was issuing a warrant prohibited by Rule 41.

CONCLUSION

The Defendant had an expectation in his home and his computer, which remained at all times in the District of Nebraska. Government officers in the Eastern District of Virginia, through the use of intrusive software, intruded upon and searched Defendant's computer, seizing information they could not have otherwise obtained. The NIT warrant that authorized this search was signed by a Magistrate who had no authority to permit searches outside of that court's district. This violation of Rule 41 rendered the warrant void from the outset, as to any searches or seizures occurring outside of the district of Virginia. A warrant that is void cannot be excused by the good-faith exception. Even if analyzed under *Leon*, the government's actions cannot be considered to have been conducted in good-faith and suppression is the appropriate remedy.

For the foregoing reasons, this Honorable Court should reject the Magistrate Judge's Findings, Recommendation and Order and sustain Defendant's Motion to Suppress.

DOMINIC DZWONCZYK, Defendant,

BY: /s/ Jim K. McGough
Jim K. McGough
Nebraska State Bar Number 21194
McGoughLaw P.C., L.L.O.
11920 Burt Street, Suite 100
PO Box 540186
Omaha, NE 68154
(402) 614-8655
jmcough@mcgoughlaw.com

CERTIFICATE OF SERVICE

I certify that on October 26, 2016, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which sent notification of such filing to the following:

Mr. Steve Russell
Assistant United States Attorney
1620 Dodge Street, Suite 1400
Omaha, NE 68102
steve.russell@usdoj.gov

/s/Jim K. McGough
Attorney for Defendant